Final version for publication in J. Number Theory.

ON EULER NUMBERS MODULO POWERS OF TWO

Zhi-Wei Sun

Department of Mathematics (and Institute of Mathematical Science)
Nanjing University, Nanjing 210093, The People's Republic of China
zwsun@nju.edu.cn
http://pweb.nju.edu.cn/zwsun

Abstract. To determine Euler numbers modulo powers of two seems to be a difficult task. In this paper we achieve this and apply the explicit congruence to give a new proof of a classical result due to M. A. Stern.

1. Introduction

Euler numbers $E_0, E_1, E_2, \ldots$ are integers given by

$$E_0 = 1 \ \text{ and } \ E_n = -\sum_{\substack{k=0\\2|n-k}}^{n-1}\binom{n}{k}E_k \text{ for } n \in \mathbb{Z}^+ = \{1,2,3,\ldots\}.$$

It is well known that $E_{2n+1} = 0$ for each $n \in \mathbb{N} = \{0,1,2,\ldots\}$ and

$$\sec x = \sum_{n=0}^{\infty}(-1)^n E_{2n}\frac{x^{2n}}{(2n)!} \quad \left(|x| < \frac{\pi}{2}\right).$$

The Euler polynomial $E_n(x)$ of degree n is defined by

$$E_n(x) = \sum_{k=0}^{n}\binom{n}{k}\frac{E_k}{2^k}\left(x-\frac{1}{2}\right)^{n-k}.$$

Clearly $E_n = 2^n E_n(1/2)$. That $E_n(x) + E_n(x+1) = 2x^n$ is a well-known fact. [Su3] contains some symmetric identities for Euler polynomials.

Euler numbers modulo an odd integer are trivial. In fact, for any $k \in \mathbb{N}$ and $q \in \mathbb{Z}^+$ we have

$$2^k E_k\left(q+\frac{1}{2}\right) = 2^k\sum_{l=0}^{k}\binom{k}{l}\frac{E_l}{2^l}q^{k-l} \equiv E_k = 2^k E_k\left(\frac{1}{2}\right) \pmod q$$

2000 *Mathematics Subject Classification*. Primary 11B68; Secondary 11A07, 11S05.

The author is supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) and the Key Program of NSF (No. 10331020) in P. R. China.

and

$$\begin{aligned}&E_k\left(\frac{1}{2}\right)-(-1)^qE_k\left(q+\frac{1}{2}\right)\\=&\sum_{j=0}^{q-1}\left((-1)^jE_k\left(j+\frac{1}{2}\right)-(-1)^{j+1}E_k\left(j+1+\frac{1}{2}\right)\right)\\=&2\sum_{j=0}^{q-1}(-1)^j\left(j+\frac{1}{2}\right)^k,\end{aligned}$$

therefore

$$E_k\equiv\sum_{j=0}^{q-1}(-1)^j(2j+1)^k\pmod q\quad\text{ providing }2\nmid q.\tag{1.1}$$

It is natural to determine Euler numbers modulo powers of two. However, this is a difficult task since $1/2$ is not a 2-adic integer. As far as the author knows, no one else has achieved this before.

In this paper we determine Euler numbers modulo powers of two in the following explicit way.

Theorem 1.1. *Let $n\in\mathbb{Z}^+$. If $k\in\mathbb{N}$ is even, then*

$$\frac{3^{k+1}+1}{4}E_k\equiv\frac{3^k}{2}\sum_{j=0}^{2^n-1}(-1)^{j-1}(2j+1)^k\left\lfloor\frac{3j+1}{2^n}\right\rfloor\pmod{2^n}\tag{1.2}$$

where $\lfloor\alpha\rfloor$ denotes the greatest integer not exceeding a real number α, moreover for any positive odd integer m we have the congruence

$$\begin{aligned}&\frac{m^{k+1}-(-1)^{(m-1)/2}}{4}E_k\\\equiv&\frac{m^k}{2}\sum_{j=0}^{2^n-1}(-1)^{j-1}(2j+1)^k\left\lfloor\frac{jm+(m-1)/2}{2^n}\right\rfloor\pmod{2^n}.\end{aligned}\tag{1.3}$$

Remark 1.1. When $k\in\mathbb{N}$ is even, $3^{k+1}+1\equiv 3+1=4\pmod 8$ and so $(3^{k+1}+1)/4$ is odd.

Theorem 1.1 implies the following nice result.

Theorem 1.2. *Let $k,l\in\mathbb{N}$ be even. If $2^n\|(k-l)$ (i.e., $2^n|(k-l)$ but $2^{n+1}\nmid(k-l)$) where $n\in\mathbb{Z}^+$, then $2^n\|(E_k-E_l)$. In other words, for any $n\in\mathbb{Z}^+$ we have*

$$E_k\equiv E_l\pmod{2^n}\iff k\equiv l\pmod{2^n}.\tag{1.4}$$

Remark 1.2. Theorem 1.2 does not tell us how to determine $E_k \bmod 2^n$ with $0 \leqslant k < 2^n$. In 1875 Stern [S] gave a brief sketch of a proof of Theorem 1.2, then Frobenius amplified Stern's sketch in 1910. In 1979 Ernvall [E] said that he could not understand Frobenius' proof and provided his own proof involving umbral calculus. Recently an induction proof of Theorem 1.2 was given by Wagstaff [W].

In the next section we will provide some lemmas. Theorems 1.1 and 1.2 will be proved in Section 3.

Now we introduce some notations throughout this paper. For $a, b \in \mathbb{Z}$ by (a, b) we mean the greatest common divisor of a and b. For an integer $q > 1$, we use $\mathbb{Z}_q$ to denote the ring of rational q-adic integers (see [M] for an introduction to q-adic numbers); those numbers in $\mathbb{Z}_q$ are simply called *q-integers* and they have the form a/b with $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ and $(a, b) = (b, q) = 1$. For $\alpha, \beta \in \mathbb{Z}_q$, by $\alpha \equiv \beta \pmod q$ we mean that $\alpha - \beta = q\gamma$ for some $\gamma \in \mathbb{Z}_q$. Two polynomials in $\mathbb{Z}_q[x]$ are said to be congruent modulo q if all the corresponding coefficients in the two polynomials are congruent mod q.

Bernoulli numbers $B_0, B_1, B_2, \ldots$ given by $B_0 = 1$ and the recursion

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0 \quad (n = 1, 2, 3, \ldots)$$

are closely related to Euler numbers.

Let $k \in \mathbb{Z}^+$ be even, and let p be an odd prime with $p - 1 \nmid k$. In 1851 E. Kummer showed that $B_k/k \in \mathbb{Z}_p$, and $B_k/k \equiv B_l/l \pmod{p^n}$ (where $n \in \mathbb{Z}^+$) for any $l \in \mathbb{Z}^+$ with $k \equiv l \pmod{\varphi(p^n)}$, where φ is Euler's totient function. In contrast with Theorem 1.2, the converse of Kummer's congruences is not true, e.g.,

$$\frac{B_{16}}{16} \equiv \frac{B_4}{4} \pmod{13^2} \quad \text{but } 16 \not\equiv 4 \pmod{\varphi(13^2)}.$$

Suppose that $p^n \| k$ where $n \in \mathbb{N}$. Then p^n divides the numerator of B_k since p does not divide the denominator of B_k by the von Staudt–Clausen theorem (cf. [IR, p. 233]). In [T] this trivial observation was attributed to J. C. Adams. Recently R. Thangadurai [T] conjectured that if $n > 0$ then p^{n+2} does not divide the numerator of B_k (i.e., $B_k/k \notin p^2\mathbb{Z}_p$).

2. Several Lemmas

For each $n \in \mathbb{N}$ the Bernoulli polynomial $B_n(x)$ of degree n is given by

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}.$$

A useful multiplication formula of Raabe asserts that

$$m^{n-1}\sum_{r=0}^{m-1}B_n\left(\frac{x+r}{m}\right)=B_n(x)\ \text{ for any } m\in\mathbb{Z}^+.$$

Euler polynomials are related to Bernoulli polynomials in the following manner:

$$\begin{aligned}\frac{n+1}{2}E_n(x)=&B_{n+1}(x)-2^{n+1}B_{n+1}\left(\frac{x}{2}\right)\\=&2^{n+1}B_{n+1}\left(\frac{x+1}{2}\right)-B_{n+1}(x).\end{aligned}\tag{2.1}$$

Lemma 2.1 ([Su2, Cor. 1.3]). *Let $a\in\mathbb{Z}$ and $k,m\in\mathbb{Z}^+$. Let $q>1$ be an integer relatively prime to m. Then*

$$\begin{aligned}&\frac{1}{k}\left(m^kB_k\left(\frac{x+a}{m}\right)-B_k(x)\right)\\\equiv&\sum_{j=0}^{q-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^{k-1}\pmod q.\end{aligned}\tag{2.2}$$

Remark 2.1. If $q>1$ is an integer relatively prime to $m\in\mathbb{Z}$, then $(1-m)/2\in\mathbb{Z}_q$ because q or m is odd.

Lemma 2.2. *Let $a\in\mathbb{Z}$, $k\in\mathbb{N}$ and $m\in\mathbb{Z}^+$. Let $q\in\mathbb{Z}^+$, $2\mid q$ and $(m,q)=1$. Then*

$$\begin{aligned}&\frac{m^{k+1}}{2}E_k\left(\frac{x+a}{m}\right)-\frac{(-1)^a}{2}E_k(x)\\\equiv&\sum_{j=0}^{q-1}(-1)^{j-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^k\pmod q.\end{aligned}\tag{2.3}$$

Proof. Let us first handle the case $4\mid q$. Denote by $\{a\}_2$ the least nonnegative residue of a modulo 2 and set $\bar{x}=(x+\{a\}_2)/2$. In view of (2.1) we have

$$\begin{aligned}&\frac{m^{k+1}}{2}E_k\left(\frac{x+a}{m}\right)-\frac{(-1)^a}{2}E_k(x)\\=&\frac{m^{k+1}}{k+1}\left(B_{k+1}\left(\frac{x+a}{m}\right)-2^{k+1}B_{k+1}\left(\frac{x+a}{2m}\right)\right)\\&-\frac{1}{k+1}\left(B_{k+1}(x)-2^{k+1}B_{k+1}(\bar{x})\right)\\=&\frac{1}{k+1}\left(m^{k+1}B_{k+1}\left(\frac{x+a}{m}\right)-B_{k+1}(x)\right)\\&-\frac{2^{k+1}}{k+1}\left(m^{k+1}B_{k+1}\left(\frac{\bar{x}+\lfloor a/2\rfloor}{m}\right)-B_{k+1}(\bar{x})\right).\end{aligned}$$

Let $P(t)$ denote the polynomial

$$\frac{1}{k+1}\left(m^{k+1}B_{k+1}\left(\frac{t+\lfloor a/2\rfloor}{m}\right)-B_{k+1}(t)\right)$$
$$-\sum_{j=0}^{q/2-1}\left(\left\lfloor\frac{\lfloor a/2\rfloor+jm}{q/2}\right\rfloor+\frac{1-m}{2}\right)\left(t+\left\lfloor\frac{a}{2}\right\rfloor+jm\right)^k.$$

Clearly $\deg P(t)\leqslant k$. Recall that $4\mid q$. By Lemma 2.1, we can write

$$P(t)=\sum_{i=0}^{k}\frac{q}{2}c_it^i\quad\text{where } c_i\in\mathbb{Z}_{q/2}=\mathbb{Z}_q.$$

Thus

$$\frac{2^{k+1}P(\bar{x})}{q}=\sum_{i=0}^{k}c_i2^k\left(\frac{x+\{a\}_2}{2}\right)^i\in\mathbb{Z}_q[x].$$

In light of the above,

$$\begin{aligned}
&\frac{m^{k+1}}{2}E_k\left(\frac{x+a}{m}\right)-\frac{(-1)^a}{2}E_k(x)\\
\equiv&\frac{1}{k+1}\left(m^{k+1}B_{k+1}\left(\frac{x+a}{m}\right)-B_{k+1}(x)\right)\\
&-2^{k+1}\sum_{j=0}^{q/2-1}\left(\left\lfloor\frac{a/2+jm}{q/2}\right\rfloor+\frac{1-m}{2}\right)\left(\bar{x}+\left\lfloor\frac{a}{2}\right\rfloor+jm\right)^k\\
\equiv&\sum_{j=0}^{q-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^k\\
&-2\sum_{\substack{i=0\\2\mid i}}^{q-1}\left(\left\lfloor\frac{a+im}{q}\right\rfloor+\frac{1-m}{2}\right)(x+a+im)^k\\
\equiv&\sum_{j=0}^{q-1}(-1)^{j-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^k\pmod q.
\end{aligned}$$

Therefore (2.3) holds.

Now we consider the remaining case $2\|q$. As $4\mid 2q$ and $(m,2q)=1$, by

the above we have

$$\begin{aligned}&\frac{m^{k+1}}{2}E_k\left(\frac{x+a}{m}\right)-\frac{(-1)^a}{2}E_k(x)\\&\equiv\sum_{j=0}^{2q-1}(-1)^{j-1}\left(\left\lfloor\frac{a+jm}{2q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^k\pmod{2q}\\&\equiv\sum_{j=0}^{q-1}(-1)^{j-1}\left(\left\lfloor\frac{a+jm}{2q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^k\\&\quad+\sum_{j=0}^{q-1}(-1)^{j+q-1}\left(\left\lfloor\frac{a+(j+q)m}{2q}\right\rfloor+\frac{1-m}{2}\right)(x+a+jm)^k\pmod q\\&\equiv\sum_{j=0}^{q-1}(-1)^{j-1}\left(a_j+\frac{1-m}{2}\right)(x+a+jm)^k\pmod q,\end{aligned}$$

where

$$\begin{aligned}a_j&=\left\lfloor\frac{a+jm}{2q}\right\rfloor+\left\lfloor\frac{a+jm+q}{2q}\right\rfloor\\&=\left\lfloor\frac{(a+jm)/q}{2}\right\rfloor+\left\lfloor\frac{(a+jm)/q+1}{2}\right\rfloor=\left\lfloor\frac{a+jm}{q}\right\rfloor.\end{aligned}$$

This completes the proof. □

Lemma 2.3. *Let $a\in\mathbb{Z}$, $m,q\in\mathbb{Z}^+$, $2\mid q$ and $(m,q)=1$. Then*

$$\sum_{j=0}^{q-1}(-1)^{j-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)=\frac{m-(-1)^a}{2}.\tag{2.4}$$

Proof. Observe that

$$\begin{aligned}&\sum_{j=0}^{q-1}(-1)^j\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)\\=&2\sum_{\substack{j=0\\2\mid j}}^{q-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)-\sum_{j=0}^{q-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)\\=&2\sum_{i=0}^{q/2-1}\left(\left\lfloor\frac{a/2+im}{q/2}\right\rfloor+\frac{1-m}{2}\right)-\sum_{j=0}^{q-1}\left(\left\lfloor\frac{a+jm}{q}\right\rfloor+\frac{1-m}{2}\right)\\=&2\left(\left\lfloor\frac{a}{2}\right\rfloor+\frac{1-m}{2}\right)-\left(\lfloor a\rfloor+\frac{1-m}{2}\right)\text{ (by [Su1, Prop. 2.1])}\\=&2\left\lfloor\frac{a}{2}\right\rfloor-a+\frac{1-m}{2}=\frac{(-1)^a-m}{2}.\end{aligned}$$

This proves (2.4). □

3. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. Obviously (1.2) follows from (1.3) in the case $m = 3$.

Let $m \in \{1, 3, 5, \ldots\}$ and $a = (m-1)/2$. Applying Lemma 2.2 with $q = 2^n$, we find that the polynomial

$$\begin{aligned} f(x) :=& \frac{m^{k+1}}{2} E_k\left(\frac{x+a}{m}\right) - \frac{(-1)^a}{2} E_k(x) \\ &+ \sum_{j=0}^{2^n-1} (-1)^j \left(\left\lfloor \frac{a+jm}{2^n} \right\rfloor + \frac{1-m}{2} \right) (x+a+jm)^k \end{aligned}$$

belongs to $2^n\mathbb{Z}_{2^n}[x]$. Observe that the coefficient of x^k in $f(x)$ is zero because

$$\frac{m^{k+1}}{2}\left(\frac{1}{m}\right)^k - \frac{(-1)^a}{2} + \sum_{j=0}^{2^n-1} (-1)^j \left(\left\lfloor \frac{a+jm}{2^n} \right\rfloor + \frac{1-m}{2} \right) = 0$$

by Lemma 2.3. So $\deg f(x) \leqslant k-1$ and hence $2^{k-1} f(x/2) \in 2^n\mathbb{Z}_{2^n}[x]$. (Note that $f(x) = 0$ if $k = 0$.) In particular, $2^{k-1} f(1/2) \equiv 0 \pmod{2^n}$.

Clearly

$$\begin{aligned} 2^{k-1} f\left(\frac{1}{2}\right) =& \frac{m^{k+1}}{2} 2^{k-1} E_k\left(\frac{1}{2}\right) - \frac{(-1)^a}{2} 2^{k-1} E_k\left(\frac{1}{2}\right) \\ &+ 2^{k-1} \sum_{j=0}^{2^n-1} (-1)^j \left(\left\lfloor \frac{a+jm}{2^n} \right\rfloor + \frac{1-m}{2} \right) \left(\frac{m}{2} + jm\right)^k \end{aligned}$$

and thus

$$\begin{aligned} & 2^{k-1} f\left(\frac{1}{2}\right) - \frac{m^{k+1} - (-1)^{(m-1)/2}}{4} E_k \\ =& \frac{m^k}{2} \sum_{j=0}^{2^n-1} (-1)^j \left(\left\lfloor \frac{jm + (m-1)/2}{2^n} \right\rfloor + \frac{1-m}{2} \right) (2j+1)^k. \end{aligned}$$

So it remains to show

$$\sum_{j=0}^{2^n-1} (-1)^j (2j+1)^k \equiv 0 \pmod{2^{n+1}} \quad \text{providing } 2 \mid k.$$

In fact,

$$\begin{aligned} & \sum_{j=0}^{2^n-1} (-1)^j (2j+1)^k = \sum_{i=0}^{2^n-1} (-1)^{2^n-1-i} \left(2(2^n-1-i)+1\right)^k \\ \equiv & - \sum_{i=0}^{2^n-1} (-1)^i \left((2^{n+1}-2i-1)^2\right)^{k/2} \equiv - \sum_{i=0}^{2^n-1} (-1)^i (2i+1)^k \pmod{2^{n+2}}. \end{aligned}$$

This concludes the proof. □

Proof of Theorem 1.2. Suppose that $k-l=2^nq$ where $n,q\in\mathbb{Z}^+$ and $2\nmid q$. We want to show $2^n\|(E_k-E_l)$.

By elementary number theory, $a^{2^n}\equiv 1\pmod{2^{n+2}}$ for any odd integer a (cf. [IR, pp. 43–44]). This, together with Theorem 1.1, yields that

$$\frac{3^{k+1}+1}{4}E_k\equiv\frac{3^k}{2}\sum_{j=0}^{2^{n+1}-1}(-1)^{j-1}(2j+1)^k\left\lfloor\frac{3j+1}{2^{n+1}}\right\rfloor$$

$$\equiv\frac{3^l}{2}\sum_{j=0}^{2^{n+1}-1}(-1)^{j-1}(2j+1)^l\left\lfloor\frac{3j+1}{2^{n+1}}\right\rfloor\equiv\frac{3^{l+1}+1}{4}E_l\pmod{2^{n+1}}.$$

As $3^k\equiv 3^l\pmod{2^{n+2}}$, the odd integers $(3^{k+1}+1)/4$ and $(3^{l+1}+1)/4$ are congruent modulo 2^n. Therefore $E_k\equiv E_l\pmod{2^n}$.

By Theorem 1.1,

$$\frac{3^{k+1}+1}{4}E_k\equiv\frac{3^k}{2}\sum_{j=0}^{1}(-1)^{j-1}(2j+1)^k\left\lfloor\frac{3j+1}{2}\right\rfloor=3^{2k}\equiv 1\pmod 2.$$

So E_k is odd. Similarly, $E_l\equiv 1\pmod 2$. In light of the above,

$$\begin{aligned}E_k\equiv E_l\pmod{2^{n+1}}&\iff\frac{3^{k+1}+1}{4}\equiv\frac{3^{l+1}+1}{4}\pmod{2^{n+1}}\\&\iff 3^{2^nq}\equiv 1\pmod{2^{n+3}}.\end{aligned}$$

It is well known that the order of 5 mod 2^{n+3} is 2^{n+1} and that $3\equiv(-1)^a5^b\pmod{2^{n+3}}$ for some $a\in\{0,1\}$ and $b\in\{0,1,\ldots,2^{n+1}-1\}$ (cf. [IR, pp. 43–44]). Thus

$$3^{2^nq}\equiv 1\pmod{2^{n+3}}\iff 5^{2^nbq}\equiv 1\pmod{2^{n+3}}\iff 2\mid bq\iff 2\mid b.$$

If $2\mid b$, then $(-1)^a3\equiv 5^b\equiv 1\pmod 8$ which is impossible. So $2\nmid b$ and hence $2^{n+1}\nmid(E_k-E_l)$. We are done. □

Acknowledgment. The author thanks Prof. Wagstaff for his information on the history of Theorem 1.2 which was rediscovered by the author.

References

[E] R. Ernvall, *Generalized Bernoulli numbers, generalized irregular primes, and class number*, Ann. Univ. Turku. Ser. A, I(178), 1979, 72 pp.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in mathematics; 84), 2nd Edition, Springer-Verlag, New York, 1990.

[M] K. Mahler, *Introduction to p-adic Numbers and their Functions*, Cambridge Univ. Press, Cambridge, 1973.

[S] M. A. Stern, *Zur Theorie der Eulerschen Zahlen*, J. Reine Angew. Math. **79** (1875), 67–98.

[Su1] Z. W. Sun, *Products of binomial coefficients modulo p^2*, Acta Arith. **97** (2001), 87–98.

[Su2] Z. W. Sun, *General congruences for Bernoulli polynomials*, Discrete Math. **262** (2003), 253–276.

[Su3] Z. W. Sun, *Combinatorial identities in dual sequences*, European J. Combin. **24** (2003), 709–718.

[T] R. Thangadurai, *Adams theorem on Bernoulli numbers revisited*, J. Number Theory **106** (2004), 169–177.

[W] S. S. Wagstaff, Jr., *Prime divisors of the Bernoulli and Euler numbers*, in: Number Theory for the Millennium, III (Urbana, IL, 2000), 357–374, A K Peters, Natick, MA, 2002.